An encrypted access key may be distributed in a number of ways. In one embodiment, the DDS subscriptions module 805 might send a message to the caster corresponding to the network area in which the purchasing user is currently located. The message could include the encrypted access key, metadata including a customer number and an indication that a key is included, and a request that the key and metadata be transmitted over the wireless link. The caster could take steps analogous to those described above to comply with the request. The terminal filter module could watch for the key by monitoring for packets whose metadata stated the customer's user ID and that a key was being transmitted. Alternately, the key could be transmitted via an alternate link such as by GSM.

In a preferred embodiment, a custom form of the IPSEC protocol is used in deincapsulation at the client terminal. According to the standard IPSEC protocol known in the art (see Fig. 10) decryption of the data payload of IP packets requires the use of a decrypted or unencrypted access key. This would require that the decrypted or unencrypted access key be stored on the terminal, and offers a high potential for piracy because the access key could be downloaded off the terminal and distributed to non-paying users.

This problem is addressed by use of the custom IPSEC protocol of an embodiment of the present invention. As seen in fig. 11, according to this custom protocol the code for decrypting the access key 1003 with the user key 1001 and terminal key 1005 is part of the IPSEC handling code. Therefore, instead of first decrypting the access key 1005 and then feeding this key to the IPSEC handling code, the access key, user key, and the terminal key are simultaneously applied to the custom IPSEC handling code. The custom IPSEC handling code decrypts the access key using its own internal decryption code and then applies the resultant decrypted key to decrypt the payload of the IP packets. In certain embodiments, the resultant decrypted key may be destroyed immediately after its application using data destruction

techniques known in the art. Furthermore, in certain embodiments the custom IPSEC handling code simultaneously decrypts the access key and uses it to decrypt the packet payloads.

As alluded to above, this method helps avoid piracy by keeping the decrypted access key from existing in an accessible storage area on the device. According to certain embodiments of the invention, all encrypted access keys that the user is in possession of are simultaneously applied to the IPSEC handling code along with the user key and terminal key. In other embodiments, the terminal would apply only one encrypted access key at a time. In such an embodiment the terminal could be notified of , or be able to determine, the appropriate key to use. Alternately, the terminal could apply all possessed encrypted access keys in succession.

It has been described herein that a user may purchase a subscription upon attempting to select a content item from the offerings list that requires a subscription that the user does not possess. Alternately, a user might select from the interface of her terminal the command "purchase subscriptions." Selection of this command could cause the terminal subscriptions module to consult its associated store to determine which of the subscriptions that the user is eligible to purchase that the user has not yet purchased. The subscriptions module may then cause the display of the terminal to list a menu noting the name, price, and/or a short description of each not-purchased subscription. The user could then select from the screen the subscription she wished to purchase. Handling of the user's purchase selections could be handled as above.

Content Voting

According to one embodiment of the present invention, users may be able to vote among several content selections for what will be transmitted over the wireless link

For example, a content provider might reserve transmission bandwidth with the scheduling intelligence module as described above, but further indicate that users should choose

from among two or more indicated selections for the actual transmission. In some embodiments the content provider would be asked to upload to the DDS all possible selections.

In certain embodiments, the scheduling intelligence module might have service announcements sent out such that a certain selection in the terminal offerings list could indicate:

> "*** Saturday Night Sci-Fi Cinema ***
>
> Vote for your choice as to which film will be transmitted at 8 p.m. this Saturday. Voting ends Wednesday at midnight. The choices are:
>
> o Star Wars
> o Star Trek II
> o Star Trek IV"

A user's selection could be sent over a GSM or other bi-directional link as a message to the scheduling intelligence module 1217. In certain embodiments, the message would additionally include an identifier such as the user's customer number. At the end of voting, Wednesday at midnight in this example, the scheduling intelligence module would tally the received votes to determine the winner. In embodiments which forwarded a unique identifier, the scheduling intelligence module would monitor for multiple votes from one individual by checking the user IDs associated with incoming votes. Duplicate votes could be dealt with by not counting any of them, only counting the first, or by implementing some other policy. However, it is noted that in certain embodiments a user may be allowed to vote for more than one content item. For example, in an alternate embodiment the above example would allow the user to vote for which two of Star Wars, Star Trek II, and Star Trek IV should be shown back-to-back as a double feature.

Furthermore, in certain embodiments, votes may be used to determine the order in which content items are transmitted. Therefore, in an alternate embodiment above example would ask a user to vote as to which of the three films she would like to see first. Once all votes